

p, q are distinct odd primes. Consider a modified RSA scheme where we define:

$$\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)}$$
 and the congruence we must satisfy is: $ab \equiv 1 \pmod{\lambda(n)}$

recall the definition of encoding/decoding functions:

$$e_k(x) = x^b \pmod{n}$$
 and $d_k(y) = y^a \pmod{n}$

we want to show that $d_k(e_k(x)) = x$

I'm assuming $x \in Z_n^*$ after some simplification we find we must show that: $x^{ab} \equiv x \pmod{n}$

since $n = pq$ where p, q distinct prime, the chinese remainder theorem allows us prove for p, q , individually:

$x^{ab} \equiv x \pmod{p}$ and $x^{ab} \equiv x \pmod{q}$ we will consider the case for mod p

since we know, for some positive integer k that: $ab = k \cdot \lambda(n) + 1$
we can reduce this to $x^{ab} \equiv (x^{\lambda(n)})^k x \pmod{n}$

next we expand: $\lambda(n) = \frac{pq-p+1}{\gcd(p-1, q-1)}$ plugging this in:

$$x^{ab} \equiv (x^{\frac{kpq}{\gcd(p-1, q-1)}})(x^{\frac{-kq}{\gcd(p-1, q-1)}})(x^{\frac{-kp}{\gcd(p-1, q-1)}})(x^{\frac{k}{\gcd(p-1, q-1)}})x \pmod{p}$$

re-arranging this:

$$x^{ab} \equiv (x^p)^{\frac{kq}{\gcd(p-1, q-1)}}(x)^{\frac{-kq}{\gcd(p-1, q-1)}}(x^p)^{\frac{-k}{\gcd(p-1, q-1)}}(x)^{\frac{k}{\gcd(p-1, q-1)}}x \pmod{p}$$

Now since p is prime, we can use fermats little theorem that says for any integer t : $t^p \equiv t \pmod{p}$ Thus we have:

$$x^{ab} \equiv (x)^{\frac{kq}{\gcd(p-1, q-1)}}(x)^{\frac{-kq}{\gcd(p-1, q-1)}}(x)^{\frac{-k}{\gcd(p-1, q-1)}}(x)^{\frac{k}{\gcd(p-1, q-1)}}x \pmod{p}$$

Cancelling the terms we have then:

$$x^{ab} \equiv x \pmod{p}$$

The proof is the same for mod q , the combination of these two with the CRT prove the overall problem.